ESP Header Compression (EHC)

draft-mglt-ipsecme-diet-esp-07
Tobias Guggemos
lpwan@IETF 104
26.03.2019
Problems when compressing

Example of an IP Tunnel

- Compression usually takes place between L2 and L3
- At that time, ESP payload is already encrypted

⇒ Only ESP header can be compressed without touching the ESP implementation
# ESP Header Compression

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>9</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

---

**Example of an IP Tunnel**

- Is already in the IPsec SA
- Can be calculated

---

Tobias Guggemos

ESP Header Compression (EHC)
ESP Header Compression (EHC)

- IPsec already has a static state (IPsec SAs)
- IPsec already has a separate channel to agree on (and update) a state
  - IKEv2, G-IKEv2, (even HIP could be used)
  - Static
- The state already holds some context (Traffic Selector)
- We have done this before (ROHCoverIPsec RFC5856)

- We just need to define how to make use of it!
EHC Actions and Rules

- Inspired from ROHC and SCHC
- Defined for ESP/IPv6/IPv4/TCP/UDP/UDP-Lite
- EHC Strategy Diet-ESP is designed to optimize context exchange
- Compressing 44 header fields with 9 context values